# 2 Забазпечення комп'ютерної безпеки в інформаційних системах

**УДК 004.056; 621.391**

## ВИКОРИСТАННЯ АВС АНАЛІЗУ ДЛЯ ОПТИМІЗАЦІЇ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

***Володимир Кононович, Юрій Копитін****
*Академія зв'язку України, *Одеська національна академія зв'язку ім. О. С. Попова*

*Анотація:* **Показана можливість використання методу АВС аналізу в питаннях захисту інформації. Продемонстровано застосування АВС аналізу для вибору комплексу засобів захисту від несанкціонованого доступу.**
*Summary* **The article shows the possibility to use the method of ABC analysis for the information protection. It demonstrates the way ABC analysis can be used to select a trusted computing base against an unauthorized access.**
*Ключові слова:* **АВС аналіз, захист інформації, державний інформаційний ресурс, несанкціонований доступ, менеджмент ризиків інформаційної безпеки, функціональний профіль захисту.**

### I Вступ

Інформаційні ресурси держави або суспільства в цілому, а також окремих організацій і фізичних осіб являють собою певну цінність, мають відповідне матеріальне вираження і вимагають захисту від різноманітних за своєю сутністю дій, які можуть призвести до витоку інформації, що захищається, а також несанкціонованих і ненавмисних впливів на неї. Тому останнім часом багато досліджень присвячують проблемі захисту інформації.

Тематика даної статті обумовлена: зростанням збитків, пов'язаних з втратою ресурсів внаслідок недоліків системи захисту інформації; збільшенням обсягу коштів, які необхідно витратити на створення та модернізацію систем захисту інформації; проблемами вибору засобів захисту (серед безлічі можливих) адаптованих до сучасних умов [1] та з оптимальним рівнем захищеності [2], який задовольняє політиці безпеки в системі.

Зауважимо, що абсолютно безпечних систем не існує [3]. Витрати на інформаційну безпеку уникнути неможливо, але їх можна звести до оптимального рівня, за якого система безпеки буде гарантувати належний рівень захищеності, а витрати на неї не будуть приводити до збитків. Саме тому питання вибору оптимальних систем захисту інформації набуває ще більшої ваги.

Проте задача вибору оптимальних систем захисту інформації досліджена недостатньо.

Мета статті – показати доцільність практичного застосування методу АВС аналізу [4] для вибору оптимальних, ефективних та економічно обґрунтованих систем технічного захисту інформації, для процесу менеджменту ризиком інформаційної безпеки та визначення достатнього набору послуг під час вибору функціонального профілю захисту.

### II Особливості застосування АВС аналізу в сфері технічного захисту інформації

Найбільш поширеним, простим, наочним та з достатнім степенем достовірності методом аналізу для виявлення першопричин виникнення проблем є метод АВС аналізу, одним з варіантів графічної інтерпретації якого виступає діаграма Парето.

У 1897 році італійський економіст і соціолог Вільфредо Парето виявив математичну залежність, яка показує, що блага розподіляються нерівномірно. Його відкриття називали по-різному, у тому числі принципом Парето, законом Парето, правилом 80/20, принципом найменшого зусилля, принципом дисбалансу. Ця ж теорія була графічно проілюстрована в 1907 р. американським економістом Максом Отто Лоренцо. Обидва вчених показали, що в більшості випадків найбільша частка благ (доходів) належить невеликій кількості людей. У 1921 графічне зображення даних, запропоноване Лоренцем, отримало назву «кривої Лоренца». Саме цим терміном прийнято називати зображення лінії, представленої на сучасних схемах АВС аналізу.

Метод "АВС аналізу" можна застосовувати практично в будь-яких галузях діяльності з метою виявлення першочергових проблем, які необхідно вирішити, шляхом визначення їхньої пріоритетності. Загальний алгоритм здійснення АВС аналізу [5] передбачає наступну послідовність дій. 1. Визначаємо мету аналізу.

2. Визначаємо об’єкти аналізу. 3. Визначаємо чинники для диференціації об'єктів аналізу. 4. Формуємо інформаційний масив для аналізу. 5. Оцінюємо об'єкти аналізу за виділеними чинниками. 6. Ранжуємо показники. 7. Здійснюємо поділ об’єктів на групи. 8. Графічно інтерпретуємо результати аналізу.

Зазначимо, що ряд авторів пропонують іншу послідовність кроків алгоритму. На нашу думку наведений вище алгоритм є найзручнішим.

У сфері технічного захисту інформації алгоритм АВС аналізу може застосовуватись на етапах побудови системи захисту інформації, які визначені ДСТУ 3396 [6, 7]. Кроки 1 – 3 алгоритму можуть виконуватись на етапі визначення й аналізу загроз, а інші кроки – на етапі розроблення системи захисту інформації. Детально даний алгоритм можна використати таким чином.

На першому кроці алгоритму чітко визначаємо мету аналізу. Наприклад: вибір оптимального набору засобів захисту, які будуть використовуватися для забезпечення безпеки об’єкта. Необхідно зазначити, що неправильно визначена мета може негативно вплинути на результати аналізу.

На другому кроці визначаємо об’єкти, які підлягають аналізу. Як об’єкти виступають: приміщення, які підлягають захисту; процеси (діяльність), які відбуваються в приміщенні; засоби захисту, які використовуються або плануються використовувати для забезпечення безпеки; інформаційні ресурси об’єкта інформаційної діяльності тощо.

На третьому кроці визначаємо чинники, на основі яких відбудеться диференціація об’єктів аналізу. За чинники приймають: потенційні загрози та їх типи; потенційні вразливості об’єкту, що захищається; необхідні витрати для побудови (модернізації) системи захисту; ймовірні ризики здійснення атаки на ресурс; вплив на виробничу здатність системи, що захищається; величина прибутку тощо.

На четвертому кроці формуємо інформаційний масив для аналізу. Для цього збираємо усі відомості за чинниками, що аналізуються. Наприклад, збираємо інформацію про потенційні загрози об’єкту, що захищається.

На п’ятому та шостому кроках проводимо: оцінку внеску кожного об’єкта за чинником, що аналізується, в загальний результат; ранжування об’єктів в порядку зменшення значення виділеного чинника; розрахунок наростаючої підсумкової частки об’єкта до загальної кількості об’єктів у відсотках та вклад об’єкта в загальний результат у відсотках.

На сьомому кроці алгоритму здійснюємо поділ отриманих результатів на групи. Даний поділ можна здійснювати за допомогою: емпіричного методу, методу суми, методу дотичних тощо. Вибір методу здійснимо далі. Число груп при проведенні АВС аналізу може бути довільним. Найбільш поширено здійснювати поділ на три групи (А: В: С). Цим і зумовлена назва методу (ABC Analysis). Зазначимо, що: групу А складає незначна кількість чинників з високим рівнем питомої ваги за обраним показником (наприклад: ресурси, які мають найбільшу ймовірність ризику здійснення атаки); групу В – середнє число чинників з середнім рівнем питомої ваги; групу С – величезна кількість чинників з незначною величиною питомої ваги.

Головний сенс дослідження у рамках АВС аналізу зводиться до того, що максимальний ефект досягається при вирішенні завдань (проблем), що відносяться до групи А. В табл. 1 наведено можливі варіанти поділу на групи за даними різних авторів [8].

Таким чином, на даний момент немає чіткого визначення границь груп в процентному співвідношенні за ступенем впливу.

Таблиця 1 – Границі груп

| Автор | Група А | Група В | Група С |
|---|---|---|---|
| Д. Дж. Бауерсокс | 80% | 15% | 5% |
| Уотерс Д. | 70% | 20% | 10% |
| Глухов В. В. | 65% | 20% | 15% |
| J. Shapiro | 60% | 20% | 20% |

Емпіричний метод передбачає поділ об’єктів на групи на основі усереднених результатів раніше проведених досліджень. Найбільш поширений варіант передбачає наступні границі: 80% внеску об’єкта до загального результату між групами А і В, та 95% – між В і С. Потім знаходимо відповідні значення частки об’єктів з загальної кількості у відсотках. Перевага методу полягає в його простоті, а недолік – в тому, що усереднені значення не завжди відповідають певній ситуації [5].

Метод «суми» передбачає виділення груп за сумою частки об’єктів із загальної кількості у відсотках (*ЧО)* та внеску об’єкта до загального результату у відсотках (*ВО*). Границя груп А та В знаходиться в точці, де сума $ЧО_A$ та $ВО_A$ дорівнюватиме 100%. Границя груп В та С – в точці, де сума $ЧО_B$ та $ВО_B$ дорівнює 145%. Зауважимо, що існують й інші варіанти визначення границь груп. Переваги методу: більш гнучкий, ніж

емпіричний метод, та краще відтворює певну ситуацію; може бути легко автоматизований. Суттєвих недоліків немає [5].

Диференційний метод передбачає що: до групи А належать об'єкти, значення чинника яких в 6 разів і більше перевищує середнє значення чиннику; до групи С – об'єкти, значення чинника за якими в 2 та більше рази менше середнього значення чинника; до групи В – усі інші об'єкти. Перевага методу полягає в його простоті, а недолік - часто призводить до некоректних результатів через невизначеність вибору коефіцієнтів. Можливий випадок, що з аналізованих об'єктів взагалі неможливо виділити групу А [5].

Метод дотичних полягає в поділі об'єктів аналізу на групи за допомогою дотичних до кривої АВС аналізу (рис. 1). Для визначення границь груп: з'єднують початок і кінець кривої прямою ОК; проводять дотичну до кривої, паралельну ОК; точка дотику М поділяє групи А і В. Далі з'єднують точки М і К та проводять дотичну до кривої, паралельну МК. Точка дотику N поділяє групи В і С. Перевага методу полягає в його гнучкості, простоті та наочності, а недолік - складність автоматизації [5].

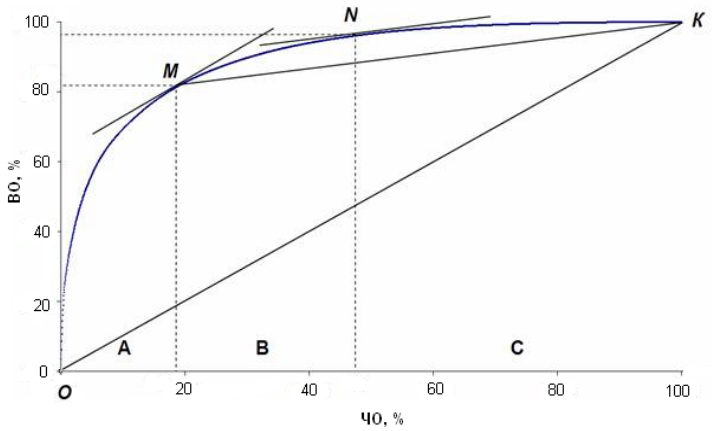


**Рисунок 1 – Метод дотичних**

Проаналізувавши різні методи проведення АВС аналізу, зупинимося на методі «суми», так як він є: більш гнучким, ніж емпіричний метод та краще відтворює певну ситуацію; одним із найпростіших і може бути легко автоматизований. Інші методи є складнішими у застосуванні.

На останньому кроці алгоритму для кращого відображення отриманих результатів здійснюємо їх інтерпретацію, шляхом побудови графіку. Такий графік називається кривою Парето, кривою Лоренца або АВС - кривою [9]. Так як АВС аналіз проводиться за методом «суми», то на осі абсцис відкладаються значення *ЧО* у відсотках, а на осі ординат відкладається значення суми *ЧО* та *ВО* у відсотках. На рис. 2 наведена графічна інтерпретація методу «суми».

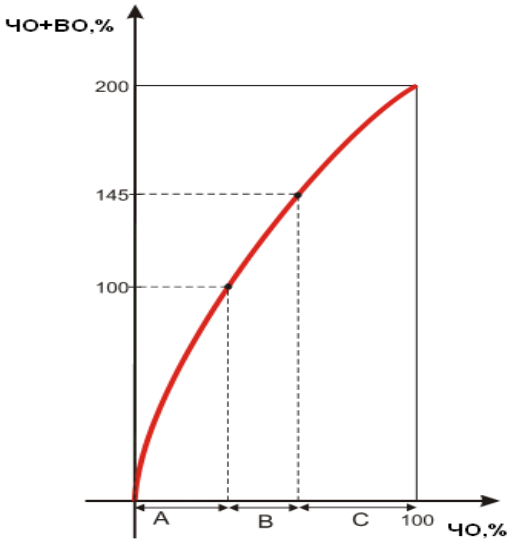


**Рисунок 2 – Графічна інтерпретація методу суми**

Далі виконуються етапи і стадії створення системи захисту, передбачені чинними нормативно-правовими документами в сфері захисту інформації.

Переваги методу АВС аналізу:

1. АВС аналіз, точний та простий у використанні, дозволяє правильно виявити основні причини проблеми для їх ефективного вирішення.

2. АВС аналіз може бути досить легко автоматизований. Теоретичні методи знаходять практичні втілення в програмних продуктах, одним з яких є продукт компанії КонСи.

Недолік методу АВС аналізу: за не чітко поставленої мети (крок 1 алгоритму) можливі неправильні висновки.

Отже, сформулюємо метод АВС аналізу стосовно питань захисту інформації: визначивши чинники, які приводять до найбільших порушень політики інформаційної безпеки, оптимізуємо витрати на забезпечення інформаційної безпеки та зменшуємо потенційні збитки, які можливо понести внаслідок недосконалості системи інформаційної безпеки, шляхом посилення заходів, спрямованих на боротьбу з цими чинниками та зменшення заходів, направлених проти менш пріоритетних чинників.

## III Використання АВС аналізу для вибору комплексу засобів захисту від несанкціонованого доступу

Розглянемо ***приклад*** використання АВС аналізу в питаннях вибору оптимального комплексу засобів захисту (КЗЗ) від несанкціонованого доступу. В даному випадку під *оптимальним* розуміється такий комплекс, який забезпечує захист від найбільш актуальних на даний момент вразливостей. Зазначимо: наведений приклад демонструє потенційну можливість використання АВС аналізу в питаннях захисту інформації. Для вибору найоптимальнішого КЗЗ необхідно здійснити комплексний всебічний аналіз всіх можливих чинників, що впливають на результат.

Для розв'язання поставленої проблеми проведемо АВС аналіз методом «суми» на базі статистики вразливостей операційних систем (ОС) за другий квартал 2008 року, наведеної в [10], та зведемо його результати в табл. 2. Зазначимо, що в [10] опубліковано 188 вразливостей, отриманих на основі 85 повідомлень від різних виробників.

Таблиця 2 – АВС аналіз вразливостей операційних систем

| Тип вразливості | Кількість вразливостей за даними [10] | Частка фактора в сумі значень фактора за даними [10], % | Наростаюче значення ВО, % | Наростаюче значення ЧО, % | Сума ЧО та ВО,% | Група |
|---|---|---|---|---|---|---|
| Відмова в обслуговуванні | 52 | 27,66 | 27,66 | 11,11 | 38,77 | A |
| Компрометація системи | 48 | 25,54 | 53,2 | 22,22 | 75,42 | A |
| Підвищення привілеїв | 44 | 23,41 | 76,61 | 33,33 | 109,94 | A |
| Обхід обмежень безпеки | 18 | 9,57 | 86,18 | 44,44 | 130,62 | B |
| Спуфінг атака | 11 | 5,85 | 92,03 | 55,55 | 147,58 | B |
| Розкриття важливих даних | 7 | 3,72 | 95,75 | 66,66 | 162,41 | C |
| Розкриття системних даних | 4 | 2,13 | 97,88 | 77,77 | 175,65 | C |
| Неавторизована зміна даних | 2 | 1,06 | 98,94 | 88,88 | 187,82 | C |
| Міжсайтовий скриптинг | 2 | 1,06 | 100 | 100 | 200 | C |

До відмови в обслуговуванні відносяться вразливості, які дозволяють зловмиснику порушити коректну роботу і вплинути на програмне застосування або ОС. До компрометації системи відносяться вразливості, які дозволяють користувачеві виконати довільний код на цільовій системі з привілеями користувача або

вразливої служби. До підвищення привілеїв відносяться вразливості, які дозволяють локальному користувачу отримати привілеї іншого облікового запису в системі.

На рис. 3 представлена АВС - крива, яка графічно інтерпретує поділ вразливостей на групи.

Виходячи з результатів, отриманих в табл. 2, першочерговими є механізми КЗЗ, які протидіють таким вразливостям як відмова в обслуговуванні, компрометація системи та підвищення привілеїв. Дані вразливості відносяться до групи А. Забезпечення захисту від трьох основних типів вразливостей знизить потенційну можливість скористатися 144 вразливостями з 188, що в відсотковому співвідношенні складає 76,61% усіх можливих вразливостей.

Для протидії відмові в обслуговуванні застосовують механізм контролю цілісності, який захищає виконувані файли від модифікації. Для протидії атакам, які пов'язані з компрометацією системи КЗЗ, застосовують механізм створення замкнутого програмного середовища. Для протидії підвищенню привілеїв – механізм ідентифікації та автентифікації.

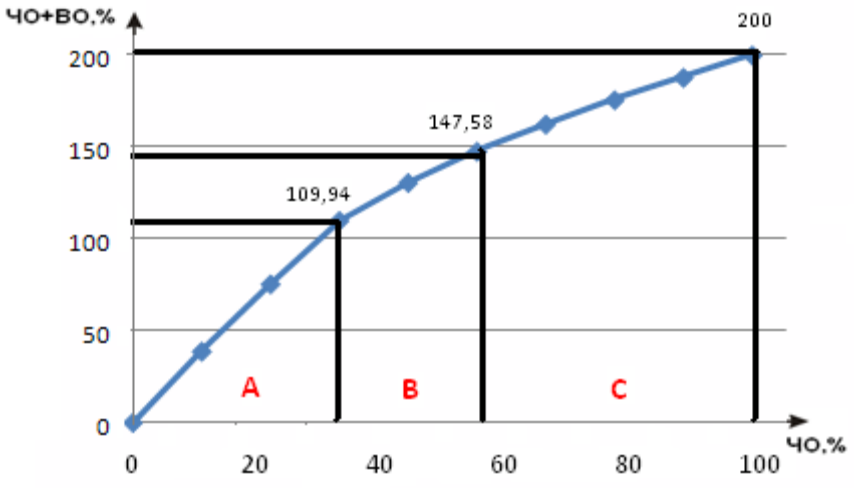


**Рисунок 3 – Графічна інтерпретація АВС аналізу**

Отже, на основі результатів проведеного аналізу можна зробити логічний підсумок, що оптимальний КЗЗ має включати такі механізми: контролю цілісності; створення замкнутого програмного середовища; ідентифікації та автентифікації. Слід зазначити, що захищаючись від атак на ці ключові вразливості за допомогою використання наведених механізмів, реалізується й захист від атак на низку інших, менш ймовірних і критичних вразливостей.

## IV Використання АВС аналізу у менеджменті ризиків інформаційної бехеки

Використання АВС аналізу в питаннях *менеджменту ризиків інформаційної безпеки*, може здійснюватись на етапі контролю функціонування та керування системою захисту інформації, визначеного ДСТУ 3396 [6, 7]. Проблем втрати таких важливих властивостей інформації як конфіденційність, цілісність та доступність уникнути неможливо. Однак ними можна керувати шляхом менеджменту ризиків – узгоджені види діяльності з керівництва та управління організацією щодо ризиків [11]. Для здійснення менеджменту ризиками використовують спеціально розроблені стандарти, методики і рекомендації. Найбільш відомі: ISO/IEC 27005, NIST 800-30, BSI, MITRE, РС БР ИББС-2.2-2009 та інші.

Процес менеджменту ризиків інформаційної безпеки представлено на рис. 4.

Авторами статі пропонується методика визначення рівня небезпеки загроз з використанням АВС аналізу для вибору ефективних захисних механізмів. Метою АВС аналізу є визначення рівня небезпеки загроз інформаційній системі для подальшого вибору ефективних захисних механізмів.

Об’єктами аналізу виступають активи інформаційної системи. До ІТ активів відносяться: інформація/дані, апаратні засоби, програмне забезпечення тощо. Повний перелік активів наведено в [12]. Як аналізований чинник виступає коефіцієнт небезпеки загрози $K_{неб}$, який обчислюється за формулою:

$$K_{неб} = \frac{\sum_{i=1}^{N} Y_i}{10 * N} \qquad (1)$$

де: $Y_i$ - значення базових показників від 1 до 10, $N$ - кількість базових показників.

До базових показників відносяться: можливість запобігання загрозі, можливість виявлення загрози, частота появи, потенційна небезпека, простота реалізації, потенційне покарання у межах діючого законодавства, ступінь захищеності від загроз тощо. Кількість показників обирається залежно від ступеня деталізації.

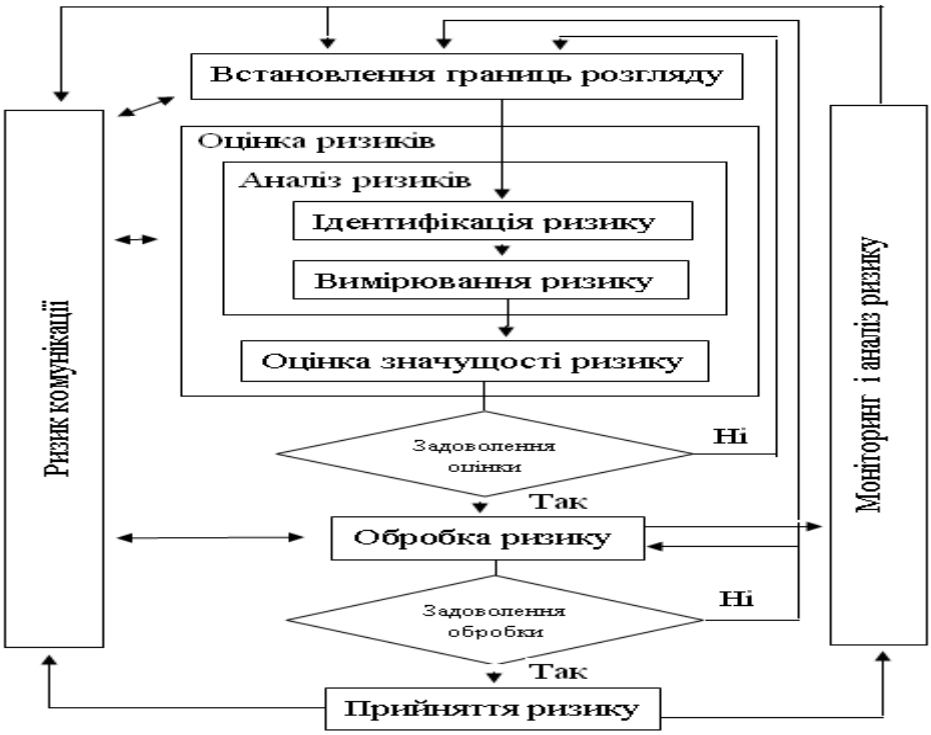


**Рисунок 4 – Процес менеджменту ризиком інформаційної безпеки (за ISO 27005 [12])**

Інформаційний масив для аналізу створюється на основі присвоєння ідентифікованим загрозам і вразливостям числових значень за базовими показниками. Для опису загроз і вразливостей використовують класифікації загроз та вразливостей (OCTAVE (США), BSI (Німеччина), DSECCT (Росія), ISO / IEC 27005 тощо).

Надалі проводиться: оцінка внеску кожного об’єкту за обраним чинником; ранжування об’єктів у порядку зменшення аналізованого чинника; обчислення наростаючого загального внеску об’єкта до загальної кількості об'єктів у відсотках і внеску об'єкта в загальний результат у відсотках.

Поділ отриманих результатів здійснюється на три групи (А, В, С). Групу А складають дуже небезпечні загрози; групу В – небезпечні загрози; групу С – безпечні. При цьому під:

- безпечними загрозами розуміються ті, яким легко запобігають або які легко виявляються, нейтралізуються та усуваються;
- небезпечними – ті, для яких процеси запобігання, виявлення і нейтралізації, з точки зору технології, не відпрацьовані;
- дуже небезпечними – ті, які мають максимальні оцінки за всіма показниками і реалізація процесів протистояння ним пов’язана з величезними витратами [13].

Сенс проведеного АВС - аналізу зводиться до того, що максимальний ефект за вибору захисних механізмів досягається при першочерговому закритті загроз, що відносяться до групи А.

Розглянемо приклад використання АВС-аналізу в процесі менеджменту ризиком інформаційної безпеки на стадії вибору захисних механізмів. Будемо вважати, що інформаційна система підприємства складається з сервера та робочої станції. Користуючись результатами обстеження об’єкта інформаційної діяльності складаємо перелік загроз та вразливостей, надаємо їм числові значення за обраними базовими показниками та обчислюємо $K_{неб}$ за формулою (1). В даному прикладі як базові показники виступають імовірність реалізації загрози та критичність реалізації загрози. Отримані результати заносимо до табл. 3. Імовірність та критичність реалізації загрози обрані на основі досвіду авторів.

Таблиця 3 – Результати обстеження об'єкта

| № з/п | Загрози | Вразливості | Імовірність реалізації загрози | Критичність реалізації загрози | Коефіцієнт небезпечності загрози |
|---|---|---|---|---|---|
| 1 | Помилки програмного забезпечення | Відсутність замкненого програмного середовища | 3 | 6 | 0,45 |
| 2 | Неправильна маршрутизація | Вільне підключення *wi-fi* обладнання | 2 | 6 | 0,4 |
| 3 | Апаратні збої | Відсутність схем резервування | 2 | 4 | 0,3 |
| 4 | Відмова в обслуговуванні | Не налаштована фільтрація | 3 | 6 | 0,45 |
| 5 | Шкідливе програмне забезпечення | Несвоєчасне оновлення баз антивірусу | 8 | 9 | 0,85 |
| 6 | НСД до інформаційної системи | Відсутність політики реагування на неправильно введений пароль | 2 | 7 | 0,45 |
| 7 | НСД до інформаційної системи | Ненадійні паролі | 3 | 7 | 0,5 |
| 8 | Крадіжка устаткування | Відсутність систем керування доступом | 7 | 6 | 0,65 |
| 9 | Зловживання інформацією | Відсутність жорстких покарань за розголошення інформації | 2 | 7 | 0,45 |
| 10 | Перехоплення ПЕМВН | Наявність неекранованих кабелів | 3 | 4 | 0,35 |
| 11 | Перехоплення інформації | Передача інформації мережею у відкритому виді | 3 | 7 | 0,5 |
| 12 | Навмисне пошкодження даних і програм | Не скрізь установлений параметр «тільки читання» | 2 | 7 | 0,45 |
| 13 | Ушкодження апаратних засобів | Відсутність спеціального приміщення для сервера | 3 | 6 | 0,45 |
| 14 | Крадіжка інформації | Відсутність реєстрації видачі на тверду копію | 2 | 6 | 0,4 |

На основі отриманого коефіцієнта небезпечності загроз проведемо АВС аналіз методом суми та занесемо отримані результати в табл. 4.

Таблиця 4 – АВС аналіз загроз обстежуваного об'єкта

| № з/п | Загрози | Вразливості | Коефіцієнт небезпечності загрози | Наростаюче значення ВО, % | Сума ЧО та ВО,% | Група |
|---|---|---|---|---|---|---|
| 5 | Шкідливе програмне забезпечення | Несвоєчасне оновлення баз антивірусу | 0,85 | 12,78 | 19,92 | А |
| 8 | Крадіжка устаткування | Відсутність систем керування доступом | 0,65 | 22,56 | 36,84 | А |
| 11 | Перехоплення інформації | Передача інформації мережею у відкритому вигляді | 0,5 | 30,08 | 51,5 | А |
| 7 | НСД до інформаційної системи | Ненадійні паролі | 0,5 | 37,59 | 66,17 | А |
| 1 | Помилки програмного забезпечення | Відсутність замкненого програмного | 0,45 | 44,36 | 80,08 | А |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | середовища | | | | |
| 4 | Відмова в обслуговуванні | Не налаштована фільтрація | 0,45 | 51,13 | 93,99 | A |
| 6 | НСД до інформаційної системи | Відсутність політики реагування на неправильно введений пароль | 0,45 | 57,89 | 107,89 | B |
| 9 | Зловживання інформацією | Відсутність строгих покарань за розголошення інформації | 0,45 | 64,66 | 121,8 | B |
| 12 | Навмисне пошкодження даних і програм | Не скрізь установлений параметр «тільки читання» | 0,45 | 71,43 | 135,71 | B |
| 13 | Пошкодження апаратних засобів | Відсутність спеціального приміщення для сервера | 0,45 | 78,2 | 149,62 | C |
| 2 | Неправильна маршрутизація | Вільне підключення wi-fi обладнання | 0,4 | 84,21 | 162,78 | C |
| 14 | Крадіжка інформації | Відсутність реєстрації видачі на тверду копію | 0,4 | 90,23 | 175,94 | C |
| 10 | Перехоплення ПЕМВН | Наявність неекранованих кабелів | 0,35 | 95,49 | 188,35 | C |
| 3 | Апаратні збої | Відсутність схем резервування | 0,3 | 100 | 200 | C |

Скориставшись результатами проведеного АВС аналізу першочергово застосуємо захисні механізми проти дуже небезпечних загроз (група А) та запишемо результати вибору захисних механізмів у табл. 5.

Таблиця 5 – Механізми протидії загрозам об’єкту обстеження

| Загрози | Вразливості | Механізми |
|---|---|---|
| Шкідливе програмне забезпечення | Несвоєчасне оновлення баз антивірусу | Включити встановлення оновлень у момент появи сигнатур |
| Крадіжка встаткування | Відсутність систем керування доступом | Встановлення ПАК з механізмом розмежування доступу |
| Перехоплення інформації | Передача інформації мережею у відкритому вигляді | Встановлення програм шифрування даних |
| НСД до інформаційної системи | Ненадійні паролі | Налаштування політики паролів |
| Помилки програмного забезпечення | Відсутність замкненого програмного середовища | Установка ПАК з механізмом замкненого ПС |
| Відмова в обслуговуванні | Не налаштована фільтрація | Установлення відповідних налаштувань брандмауера |

Даний приклад продемонстрував, що використання АВС аналізу на стадії вибору захисних заходів безпеки надає можливість значно підвищити якість менеджменту інформаційних ризиків, обрати оптимальні заходи безпеки, які забезпечують захист від небезпечних загроз для конкретного об’єкта, здійснити легко, швидко і зручно адаптацію систем захисту до умов, що змінюються.

## V Використання АВС аналізу у визначенні достатнього набору послуг функціонального профілю захисту

Розглянемо використання АВС аналізу в питаннях визначення достатнього набору послуг під час вибору функціонального профілю захисту (ФПЗ). Вимоги до функціонального складу КЗЗ залежать від

характеристик оброблюваної інформації, самої ОС, фізичного середовища, персоналу і організаційної підсистеми. Вимоги до гарантій визначаються насамперед характером (важливістю) оброблюваної інформації і призначенням автоматизованої системи (АС).

В межах кожного класу АС класифікуються на підставі вимог до забезпечення певних властивостей інформації. В зв'язку з цим в кожному класі АС виділяються підкласи. Для кожного з підкласів кожного класу вводиться деяка кількість ієрархічних стандартних функціональних профілів, яка може бути різною для кожного класу і підкласу АС. Профілі є ієрархічними в тому розумінні, що їх реалізація забезпечує наростаючу захищеність від загроз відповідного типу (конфіденційності, цілісності і доступності). Наростання ступеня захищеності може досягатись як підсиленням певних послуг, тобто включенням до профілю більш високого рівня послуги, так і включенням до профілю нових послуг.

Така класифікація корисна для полегшення вибору переліку функцій, які має реалізовувати КЗЗ ОС, проектованої або існуючої АС. Цей підхід дозволяє мінімізувати витрати на початкових етапах створення КСЗІ АС. Проте слід визнати, що для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної АС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків [14].

Стандартний функціональний профіль захищеності є переліком мінімально необхідних рівнів послуг, які має реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.

Зазначимо, що кількість та рівень послуг можуть змінюватися залежно від характеру (важливості) оброблюваної інформації і призначення АС.

Метод АВС аналізу в питаннях оптимізації функціональних послуг можна використати таким чином: спочатку провести оцінку потенційних вразливостей, та (або) рівня загроз, та (або) рівня ризику, а далі провести ранжирування з використанням АВС аналізу для визначення ступеня впливу кожної загрози (вразливості) на оцінювану систему. На основі результатів аналізу стандартний функціональний профіль можна буде залишити без змін, якщо забезпечується захист від загроз (вразливостей), що відносяться до групи А, або доповнювати послугами, які забезпечують захист від найбільш небезпечних загроз (група А) або навпаки виключати послуги в разі відсутності загроз. В результаті додавання послуг можуть виникати версії ФПЗ. Версія може служити, зокрема, для вказівки на підсилення певної послуги всередині профілю. Тим не менше, внесення деяких істотних змін, особливо додання нових послуг, може або привести до появи нового профілю, або до того, що профіль буде відноситись до іншого класу чи підкласу АС. Єдина вимога, якої слід дотримуватися при утворенні нових профілів, — це додержання описаних в НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [15] необхідних умов для кожної із послуг, що включаються до профілю.

Розглянемо приклад використання АВС-аналізу в процесі вибору ФПЗ та визначення необхідних захисних послуг АС класу 2, призначеної для автоматизації діяльності органів державної влади (ОДВ).

В автоматизованих системах, призначених для автоматизації діяльності ОДВ, обробляється інформація з обмеженим доступом. Основними загрозами для інформації в таких системах є загрози, що призводять до несанкціонованого ознайомлення з інформацією, тобто загрози (порушення) конфіденційності. У зв'язку з цим до КЗЗ ОС, що входять до складу АС, у першу чергу пред'являються вимоги щодо забезпечення конфіденційності оброблюваної інформації, персональної відповідальності користувачів за дотримання режиму секретності.

На етапі проектування КСЗІ було встановлено, що необхідно використовувати стандартний профіль 2.К.4 = { КД-2, КА-2, КО-1, КК-1, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2 }.

За допомогою АВС аналізу підтвердимо достатність послуг, які входять до даного ФПЗ, скориставшись результатами аналізу вразливостей ОС, наведених у табл. 2. Згідно з ними найбільша імовірність, що зловмисник скористається такими вразливостям як відмова в обслуговуванні, компрометація системи та підвищення привілеїв. Для протидії даним вразливостям необхідно, щоб КЗЗ реалізовував відповідно такі послуги: ДР-2 *(*недопущення захоплення ресурсів*),* ЦД-2 *(*базова довірча цілісність*),* КК-2 *(*контроль прихованих каналів*).* Тобто до запропонованого вище профілю необхідно додати такі послуги: ДР-2, ЦД-2 та підвищити КК-1 до КК-2.

Отже, для забезпечення надійного захисту КЗЗ повинен реалізовувати такі послуги { КД-2, КА-2, КО-1, КК-2, ЦД-2, ДР-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2 }.

Даний приклад продемонстрував, що використання АВС аналізу в процесі вибору ФПЗ та визначення необхідних захисних послуг надає можливість легко та зручно перевірити, чи забезпечує даний профіль належний рівень захисту від найбільш небезпечних загроз, чи його необхідно доповнювати послугами більш високого рівня або навпаки зменшувати (вилучити) певні послуги.

## VI Висновки

Використання розглянутого методу АВС аналізу в питаннях захисту інформації дозволяє швидко та зручно визначити механізми захисту, які необхідно застосовувати для підтримання належного рівня політики інформаційної безпеки. Тим самим створюються оптимізовані, ефективні та економічно обґрунтовані системи захисту інформації, оскільки основні витрати спрямовані на найбільш вразливі місця об'єкту, а інші – зменшуються за умови відсутності порушень політики безпеки. Зокрема, це вибір комплексу засобів захисту, який забезпечує захист від актуальних на даний момент вразливостей.

Використання методу АВС аналізу надає можливість надалі:

- обирати оптимальні системи захисту інформації, які забезпечують захист від актуальних загроз та вразливостей;
- створювати економічно ефективні системи захисту, які будуть гарантувати належний рівень захищеності, а витрати на неї не будуть приводити до збитків, пов'язаних з перевищенням вартості системи величини можливого отриманого прибутку від інформації, що захищається;
- здійснювати зручно та швидко адаптацію систем захисту до умов, що змінюються.

Таким чином, для вибору оптимальних, ефективних та економічно обґрунтованих систем захисту інформації доцільно застосовувати метод АВС аналізу. Напрямом подальшого дослідження може бути розробка методик використання методу АВС аналізу на етапах побудови систем захисту інформації.

*Література:* ***1.*** *Де Гроот М. Оптимальные статистические решения [Текст]: пер. с англ. / М. Де Гроот; ред. Ю. В. Линник. – М.: Мир, 1974. – 491 с.* ***2.*** *Баутов А. Экономический взгляд на проблемы информационной безопасности. [Електронний ресурс] / Баутов А.// Открытые системы – 2002. – № 2. – Режим доступу: http://www.osp.ru/os/2002/02/181118/. – Назва з екрану.* ***3.*** *Adi Shamir. Turing Award lecture [Електронний ресурс] / Adi Shamir. – 2004 – Режим доступу: http://www.financialcryptography.com/mt/archives/000147.html. – Назва з екрану.* ***4.*** *АВС-анализ [Електронний ресурс] – Режим доступу: http://www.abc-analysis.ru/. – Назва з екрану.* ***5.*** *Фишер Андрей. Методы выделения групп в АВС анализе [Електронний ресурс] / Фишер Андрей. – Режим доступу: http://www.transmap.ru/articles/view/169. – Назва з екрану.* ***6.*** *ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.* ***7.*** *ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.* ***8.*** *Методы АВС анализа номенклатурных групп [Електронний ресурс]: (По книге «Модели м методы теории Логистики», Лукинский В. С. и др.). – Режим доступу:http://www.adviss.ru/content/view/45/7/. – Назва з екрану.* ***9.*** *Аналіз АВС [Електронний ресурс]. – Режим доступу: http://www.basegroup.ru/glossary/definitions/abc_analysis/. – Назва з екрану.* ***10.*** *Отчет по уязвимостям за второй квартал 2008 года [Електронний ресурс] / Валерий Марчук. – Режим доступу: http://www.securitylab.ru. – Назва з екрану.* ***11.*** *ISO/IEC 27001:2005 Information technology – Security techniques – Specification for an Information. Security Management System.* ***12.*** *ISO/IEC 27005:2008 Information technology – Security techniques – Information security risk management.* ***13.*** *Черней Г. А. Оценка угроз безопасности автоматизированным информационным системам [Електронний ресурс]: – Режим доступа: http://security.ase.md/publ/ru/pubru01.html.* ***14.*** *НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – 16 с.* ***15.*** *НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – 57 с.*

**УДК 004.056.53**

# АВТЕНТИФИКАЦИЯ В ЗАЩИЩЕННЫХ ПРИЛОЖЕНИЯХ

***Михаил Коломыцев, Светлана Носок***

*Национальный технический университет Украины «Киевский политехнический институт»*

*Анотація:* **Наведено місце додатків в інфраструктурі комп'ютерної системи, розглянуто основні аспекти і задачі захисту додатків, проаналізовано різні способи автентифікації як засобу безпеки додатків та висвітлено загальні вимоги до реалізації механізму автентифікації.**

*Summary:* **The article outlines the place of applications in the infrastructure of computer system. The main aspects and tasks of application protection are described. Different ways of authentication as a method of application protection are analysed, and general reguirements concerning realization of authentication mechanism are mentioned.**

*Ключові слова:* **Автентифікація, додатки, операційна система, система управління базами даних.**